WHAT IS CLAIMED IS:

1. A person authentication system for executing person authentication through comparing a template serving as user identification data which has already been acquired with sampling information input by a user, said person authentication system comprising:

a person identification authority for creating a person identification certificate storing the template;

an entity which executes person authentication for comparing the template with the sampling information input by a user as person authentication on the basis of the person identification certificate; and

an entity which requests person authentication for requesting to said entity which executes person authentication for person authentication.

2. A person authentication system according to Claim 1,

wherein said entity which requests person authentication and said entity which executes person authentication are included in a user device serving as a data processing apparatus having the comparison/verification capability, and said person identification authority provides the person identification certificate storing the template that has been encrypted by a public key of said user device,

whereby said user device decrypts the encrypted template in the received person identification certificate by using a private key of said user device, and compares the decrypted template with the sampling information input by a user, thereby performing person authentication.

3. A person authentication system according to Claim 1,

wherein said entity which requests person authentication is a user device, and said entity which executes person authentication is a service provider for providing service to said user device, and said person identification authority provides the person identification certificate storing the template that has been encrypted by a public key of said service provider to said service provider,

whereby said user device provides the sampling information input by a user to said service provider, and said service provider decrypts the encrypted template in the person identification certificate received from said person identification authority by using a private key of said service provider, and compares the decrypted template with the sampling information input by a user provided from said user device, thereby performing person authentication.

4. A person authentication system according to Claim 1,

wherein said entity which requests person authentication is a user device or a service provider, and said entity which executes person authentication is said person identification authority, and said user device or said service provider provides the sampling information input by a user to said person identification authority,

whereby said person identification authority decrypts the template that has been encrypted in the person identification certificate by using a private key of said person identification authority and compares the decrypted template with the sampling information input by a user provided from said user device or said service provider, thereby performing person authentication.

5. A person authentication system according to Claim 1,

wherein said person identification authority decrypts the template that has been encrypted and stored in the person identification certificate by using a private key of said person identification authority and re-encrypts the decrypted template by using a public key of said entity which executes person authentication and stores the re-encrypted template in the person identification certificate, thereby transmitting the stored template to said entity which executes person authentication.

6. A person authentication system according to Claim 1,

wherein said person identification authority receives a public key certificate from said entity which executes person authentication and reads a public key after verifying the public key certificate and decrypts the template that has been encrypted in the person identification certificate by using a private key of said person identification authority and re-encrypts the decrypted template by using the public key of said entity which executes person authentication read from the public key certificate and stores the re-encrypted template in the person identification certificate, thereby transmitting the stored template to said entity which executes person authentication.

7. A person authentication system according to Claim 1, comprising:

a mobile terminal storing the person identification certificate,

wherein said entity which executes person authentication receives, from said mobile terminal, the person identification certificate and a key for encrypting and decrypting the template of the person identification certificate, the key that has been decrypted by using a private key of said mobile terminal, and decrypts the template stored in the received person identification certificate by using the key for encrypting and decrypting the template, thereby performing person authentication.

8. A person authentication system according to Claim 1, comprising:

a mobile terminal storing the person identification certificate,

wherein said entity which executes person authentication receives, from said mobile terminal, the template stored in the person identification certificate, the template that has been decrypted by using a private key of said mobile terminal, thereby performing person authentication on the basis of the received template.

9. A person authentication system according to Claim 1, comprising:

a mobile terminal storing the person identification certificate,

wherein said entity which executes person authentication is said mobile terminal that decrypts, by using a private key of said mobile terminal, the template that has been encrypted in the person identification certificate stored in said mobile terminal and compares the decrypted template with the sampling information input by a user, thereby performing person authentication.

10. A person authentication system according to Claim 1,

wherein said entity which requests person authentication is a user device, and said entity which executes person authentication is a service provider for providing service to said user device, and said user device provides the sampling information input by a user and the person identification certificate storing the template that has been encrypted by using a public key of said service provider to said service provider, and said service provider decrypts, by using a private key of said service provider, the template that has been encrypted in the person identification certificate received from said user device and compares the decrypted template with the sampling information input by a user provided from said user device, thereby performing person authentication.

11. A person authentication system according to Claim 1,

wherein said entity which requests person authentication is a user device, and said entity which executes person authentication is a service provider for providing service to said user device, and

said service provider verifies a signature of said person identification authority written in the person identification certificate provided by said user device and transmits the result of verification to said user device, and

said user device decrypts, by using a private key of said user device, a key for encrypting and decrypting the template, the key that has been encrypted by using a public key of said user device and stored in the person identification certificate and provides the decrypted key to said service provider, with the sampling information input by a user, on condition that the signature is verified to have never been tampered with,

whereby said service provider that is said entity which executes person authentication decrypts, by using the key for encrypting and decrypting the template, the template in the person identification certificate received from said user device, thereby performing person authentication.

12. A person authentication system according to Claim 1,

wherein said entity which requests person authentication is a user device, and said entity which executes person authentication is a service provider for providing service to said user device, and

said service provider receives the template in the person identification certificate from said user device, the template that has been decrypted by using a private key of said user device, thereby performing person authentication on the basis of the received template.

13. A person authentication system according to Claim 1,

wherein said entity which executes person authentication is a user device, and said entity which requests person authentication is a service provider for providing service to said user device,

said user device decrypts, by using a private key of said user device, the template that has been encrypted in the person identification certificate received from said person identification authority and compares the decrypted template with the sampling information input by a user, thereby performing person authentication and notifying said service provider of the result of comparison.

14. A person authentication system according to Claim 1,

wherein mutual authentication is performed between data transmission devices, and data is transmitted together with a digital signature that is verified, so as to check whether the data has been tampered with or not, in mutual data communication performed by said person identification authority, said entity which executes person authentication and said entity which requests person authentication.

15. A person authentication method for executing person authentication through comparing a template serving as user identification data which has already been acquired with sampling information input by a user, said person authentication method comprising the steps of:

creating a person identification certificate storing the template by said person identification authority;

reading out a request for person authentication from said entity which requests person authentication to said entity which executes person authentication; and

comparing the template with the sampling information input by a user as person authentication on the basis of the person identification certificate in said entity which executes person authentication.

16. A person authentication method according to Claim 15,

wherein said entity which requests person authentication and said entity which executes person authentication are included in a user device serving as a data processing apparatus having the comparison/verification capability, and said person identification authority provides the person identification certificate storing the template that has been encrypted by a public key of said user device to said user device,

whereby said user device decrypts the encrypted template in the received person identification certificate by using a private key of said user device, and compares the decrypted template with the sampling information input by a user, thereby performing person authentication.

17. A person authentication method according to Claim 15,

wherein said entity which requests person authentication is a user device, and said entity which executes person authentication is a service provider for providing service to said user device, and said person identification authority provides the person identification certificate storing the template that has been encrypted by a public key of said service provider to said service provider, and said user device provides the sampling information input by a user to said service provider,

whereby said service provider decrypts the encrypted template in the person identification certificate received from said person identification authority by using a private key of said service provider, and compares the decrypted template with the sampling information input by a user provided from said user device, thereby performing person authentication.

18. A person authentication method according to Claim 15,

wherein said entity which requests person authentication is a user device or a service provider, and said entity which executes person authentication is said person identification authority, and said user device or said service provider provides the sampling information input by a user to said person identification authority,

whereby said person identification authority decrypts, by using a private key of said person identification authority, the template that has been encrypted in the person identification certificate and compares the decrypted template with the sampling information input by a user provided from said user device or said service provider, thereby performing person authentication.

19. A person authentication method according to Claim 15,

wherein said person identification authority decrypts, by using a private key of said person identification authority, the template that has been encrypted in the person identification certificate and re-encrypts the decrypted template by using a public key of said entity which executes person authentication and stores the re-encrypted template in the person identification certificate, thereby transmitting the stored template to said entity which executes person authentication.

20. A person authentication method according to Claim 15,

wherein said person identification authority receives a public key certificate from said entity which executes person authentication and reads a public key after verifying the public key certificate and decrypts, by using a private key of said person identification authority, the template that has been encrypted in the person identification certificate and re-encrypts the decrypted template by using the public key of said entity which executes person authentication read from the public key certificate and stores the re-encrypted template in the person identification certificate, thereby transmitting the stored template to said entity which executes person authentication.

21. A person authentication method according to Claim 15,

wherein the person identification certificate is stored in a mobile terminal, and said entity which executes person authentication receives, from said mobile terminal, the person identification certificate and a key for encrypting and decrypting the template of the person identification certificate, the key that has been decrypted by using a private key of said mobile terminal, and decrypts the template in the received person identification certificate by using the key for encrypting and decrypting the template, thereby performing person authentication.

22. A person authentication method according to Claim 15,

wherein the person identification certificate is stored in a mobile terminal, and said entity which executes person authentication receives, from said mobile terminal, the template in the person identification certificate, the template that has been decrypted by using a private key of said mobile terminal, thereby performing person authentication on the basis of the received template.

23. A person authentication method according to Claim 15,

wherein the person identification certificate is stored in a mobile terminal, and said entity which executes person authentication is said mobile terminal that decrypts, by using a private key of said mobile terminal, the template that has been encrypted in the person identification certificate stored in said mobile terminal and compares the decrypted template with the sampling information input by a user, thereby performing person authentication.

24. A person authentication method according to Claim 15,

wherein said entity which requests person authentication is a user device, and said entity which executes person authentication is a service provider for providing service to said user device, and said user device provides the sampling information input by a user and the person identification certificate storing the template that has been encrypted by using a public key of said service provider to said service provider, and said service provider decrypts, by using a private key of said service provider, the template that has been encrypted in the person identification certificate received from said user device and compares the decrypted template with the sampling information input by a user provided from said user device, thereby performing person authentication.

25. A person authentication method according to Claim

15,

wherein said entity which requests person authentication is a user device, and said entity which executes person authentication is a service provider for providing service to said user device, and

said service provider verifies a signature of said person identification authority written in the person identification certificate provided by said user device and transmits the result of verification to said user device, and said user device decrypts, by using a private key of said user device, a key for encrypting and decrypting the template, the key that has been encrypted by using a public key of said user device and stored in the person identification certificate, and provides the decrypted key with the sampling information input by a user to said service provider, on condition that the signature is verified to have never been tampered with,

whereby said service provider that is said entity which executes person authentication decrypts, by using the key for encrypting and decrypting the template, the template in the person identification certificate received from said user device, thereby performing person authentication.

26. A person authentication method according to Claim 15,

wherein said entity which requests person authentication is a user device, and said entity which executes person authentication is a service provider for providing service to said user device, and

said service provider receives the template in the person identification certificate from said user device, the template that has been decrypted by using a private key of said user device, thereby performing person authentication on the basis of the received template.

27. A person authentication method according to Claim 15,

wherein said entity which executes person authentication is a user device, and said entity which requests person authentication is a service provider for providing service to said user device,

said user device decrypts, by using a private key of said user device, the template that has been encrypted in the person identification certificate received from said person identification authority, and compares the decrypted template with the sampling information input by a user, thereby performing person authentication and notifying said service provider of the result of comparison.

28. A person authentication method according to Claim

15,

wherein mutual authentication is performed between data transmission devices, and data is transmitted together with a digital signature that is verified, so as to check whether the data has been tampered with or not, in mutual data communication performed by said person identification authority, said entity which executes person authentication and said entity which requests person authentication.

29. A program providing medium for providing a computer program which is capable of performing, on a computer system, person authentication through comparing a template serving as user identification data which has already been acquired with sampling information input by a user, said computer program comprising the steps of:

reading out a request for person authentication from an entity which requests person authentication to an entity which executes person authentication; and

comparing the template with the sampling information input by a user as person authentication on the basis of a person identification certificate that has been issued by a person identification authority in accordance with the request for person authentication, in said entity which executes person authentication.